PATENT

Docket No.: 100200290-1
Appl. Ser. No.: 10/084,499

IN THE CLAIMS:

Please find below a listing of all of the pending claims. The statuses of the claims are set forth in parentheses.

1. (Currently Amended) A method for increasing peer privacy, comprising:

forming a path from a provider to a requestor by selecting a plurality of peers in response to receiving a request for information;

updating a table on each peer of said plurality of peers with a respective path index entry for said information;

transmitting a message to said requestor through said plurality of peers, said message comprising said information and a path index for said information from said provider; ~~and~~

determining a next peer according to said path for said information by searching said table of each peer of said plurality of peers with said path index as an index into said table;

retrieving an identity of said next peer according to said path for said information and a respective index peer of said next peer;

encrypting said path index with a public key of said respective index peer of said next peer to form a next state of said path index; and

transmitting a new message with said information and said next state of said path index as said path index to said next peer.

2. (Canceled).

3. (Original) The method according to claim 1, further comprising:

receiving said request for information at a directory;

determining an availability of said information; and

notifying said requestor of a determination of non-availability.

4. (Original) The method according to claim 1, further comprising:

receiving said request for information at a directory;

determining an availability of said information; and

generating an encryption key in response to a determination of said availability.

5. (Original) The method according to claim 4, further comprising:

determining a first next peer from said provider and a respective index peer for said first next peer according to said path; and

encrypting a reference to said information, said first next peer, and said respective index peer of said first next peer with said encryption key.

6. (Original) The method according to claim 5, wherein said encryption key is generated according to a DES encryption algorithm.

7. (Original) The method according to claim 5, further comprising:

encrypting said encryption key with a public key of said requestor;

encrypting said encryption key with a public key of said provider;

forming a provider message, wherein said provider message comprises:

said encryption key encrypted with said public key of said requestor;

said encryption key encrypted with said public key of said provider;

said encrypted reference; and

said encrypted first next peer and said respective first index peer; and

transmitting said message to said provider.

8. (Original) The method according to claim 1, further comprising:

forming a respective path message to each peer of said plurality of peers, said respective path message comprising said respective path index entry.

9. (Original) The method according to claim 8, wherein said respective path index entry comprises an identity of a next peer according to said path, a respective index peer for said next peer, and an index entry.

10. (Original) The method according to claim 8, wherein said identity of next peer according to said path and said respective index peer for said next peer are encrypted with a public key of a peer receiving said respective path message.

11. (Original) The method according to claim 8, wherein said index entry is formed according to $\{ public_{b_1} (...public_{b_n} (public_{b_m} (n))..)\}$, where b_j represents said respective index peer.

12. (Currently Amended) A method of transmitting information, comprising:

updating a respective table of each peer of a plurality of peers with a respective path index entry in response to receiving a path formation message containing said respective path index entry;

receiving a message comprising said information and a path index; and

forwarding said information to a next peer in response to a determination of said next peer from said table with said path index as a search index into said table;

forming a next state of said path index by encrypting said path index with a public key of a respective index peer of said next peer;

forming a new message with said information and said next state of said path index as said path index; and

transmitting said new message to said next peer.

13. (Canceled).

14. (Original) The method according to claim 12, further comprising:

determining an availability of information in response to receiving a request for information from a requestor; and

notifying said requestor of a determination of non-availability.

15. (Original) The method according to claim 12, further comprising:

determining an availability of information in response to receiving a request for information from a requestor; and

forming a path through a plurality of peers with a provider as a beginning of said path to said requestor in response to a determination of availability.

16. (Original) The method according to claim 15, further comprising:

generating an encryption key;

determining a first next peer from said provider according to said path and a respective index peer to said first next peer;

encrypting a reference to said information, said first next peer and said respective index peer with said encryption key; and

transmitting a retrieval message to said provider, said message comprises:

said encrypted reference;

said encrypted first next peer;

said encrypted respective index peer of said first next peer;

a value of a message counter for said information;

said encryption key encrypted with a public key of said provider; and

said encryption key encrypted with a public key of said requestor.

17. (Original) The method according to claim 15, wherein said generation of said encryption key utilizes a DES encryption algorithm.

18. The method according to claim 15, further comprising:

receiving said second message at said provider;

applying a complementary key to said public key of said provider to said obtain said encryption key; and

applying said encryption key to said encrypted reference to retrieve said reference.

19. (Original) The method according to claim 18, further comprising:

retrieving said information based on said decrypted reference;

encrypting said information with said encryption key;

forming said message, wherein said message comprises:

said encrypted information;

encryption key encrypted with a public key of said requestor; and

said path index formed by encrypting said value of message counter with a public key of said respective index peer of said first next peer; and

transmitting said message to said first next peer according to said path.

20. (Original) The method according to claim 12, further comprising:

receiving said message at said requestor;

applying a complementary key to said public key of said requestor to said encryption key encrypted with said public key of said requestor to obtain said encryption key;

applying said encryption key to said encrypted reference to retrieve said information.

21. (Currently Amended) A method of increasing peer privacy, comprising:

selecting a path for information from a provider to a requestor through a plurality of peers in response to a received request for said information; ~~and~~

receiving a respective set-up message at each peer of said plurality of peers, wherein said respective set-up message comprises a predetermined label and an identity of a next peer for said information according to said path;

generating an encryption key;

encrypting said encryption key with a public key of said requestor;

encrypting said encryption key with a public key of said provider; and

encrypting a transaction identifier, a reference for said information, and a first next peer according to said path with said encryption key.

22. (Original) The method according to claim 21, further comprising:

updating a table with said predetermined label and said identity of a next peer for said information according to said path.

23. (Currently Amended) The method according to claim 22, further comprising:

receiving a message, wherein said message comprises:

[[an]] said encryption key encrypted with a public key of said requestor;

said information encrypted with said encryption key; and

a message label; and

retrieving said identity of next peer from said table in response to said message label matching said predetermined label in said table.

24. (Original) The method according to claim 23, further comprising:

encrypting said label with a public key of said next peer;

reformatting said message with said label encrypted with said public key of said next peer as said label; and

transmitting said message to said next peer.

25. (Original) The method according to claim 23, further comprising:

comparing said identity of said next peer with a current peer;

decrypting said encryption key encrypted with a public key of said requestor in response to said identity of said next peer being said current peer; and

decrypting said information encrypted with said encryption key.

26. (Canceled).

27. (Currently Amended) The method according to claim [[26]] 21, further comprising:

forming a retrieval message comprising:

said encryption key encrypted with said public key of said requestor;

said encryption key encrypted with said public key of said provider;

said transaction identifier, said reference for said information, and said first next peer according to said path encrypted with said encryption key; and

transmitting said retrieval message to said provider.

28. (Original) The method according to claim 27, further comprising:

applying a complementary key of said provider to said encryption key encrypted with said public key of said provider; and

decrypting said reference for said information, said transaction identifier, and said first next peer.

29. (Original) The method according to claim 28, further comprising:

retrieving said information based on said reference for said information;

encrypting said information with said encryption key; and

forming a message label based on said transaction identifier.

30. (Original) The method according to claim 29, further comprising:

forming a message including said encrypted information and said message label; and

transmitting said message to said first next peer.

31-41. (Canceled).

42. (Currently Amended) A method of increasing peer privacy, comprising:

forming a path for information from a provider to a requestor through a plurality of peers in response to a received request for said information;

transmitting to each peer of said plurality of peers a respective set-up message comprising of a predetermined label and an identity of a next peer for said information; ~~and~~

if a label stored at an intermediate peer of the plurality of peers does not match the predetermined label in the set-up message, the intermediate peer stores the predetermined label and the corresponding identity of the next peer;

if a label stored at the intermediate peer matches the predetermined label, the intermediate peer retrieves a previously stored message and generates a next state of the predetermined label for the setup message; and

transferring said information over said path in a message by determining a next peer according to said path by matching a message label included in said message to said predetermined label.

43. (New) The method of claim 42, wherein generating a next state further comprises:

encrypting the received predetermined label with a public key of a respective index peer of the next peer.

44. (New) The method of claim 42, wherein the stored message comprises:

an encryption key encrypted with the public key of the requestor.